Mathematics 202 Combinatorics & Number Theory Solutions

Professor Peter M. Higgins

March 6, 2020

Solutions and Comments for the Problems

Problem Set 1

1. $3x \equiv 2 \pmod 6$ has no solution (because the gcd(3,6) $= 3$ does not divide 2).

2.

$$5x \equiv 2 \,(\text{mod } 6) \Rightarrow 5x \equiv 20 \,(\text{mod } 6) \Rightarrow x \equiv 4 \,(\text{mod } 6)$$

Note that since the gcd(5,6) $= 1$, there is a unique least residue solution.

3.

$$4x \equiv 2 \,(\text{mod } 6) \Rightarrow 4x \equiv 8 \,(\text{mod } 6) \Rightarrow x \equiv 2 (\text{mod } 3)$$

and there are 2 least residue solutions, they being $x = 2$ and $x = 2 + 3 = 5$.

4. Since 31 is prime, there is a unique least residue solution.

$$6x \equiv 14 \,(\text{mod } 31) \Rightarrow 3x \equiv 7 \Rightarrow 3x \equiv 69 \,(\text{mod } 31)$$

$$\Rightarrow x \equiv 23 \,(\text{mod } 31).$$

5.

$$15x \equiv 12 \,(\text{mod } 57) \Rightarrow 5x \equiv 4 \,(\text{mod } 19) \Rightarrow 5x \equiv 80 (\text{mod } 19)$$

$$\Rightarrow x \equiv 16 \,(\text{mod } 19)$$

and so the full set of least residue solutions is $\{16, 16 + 19 = 35, 35 + 19 = 54\}$.

6. $x \equiv 1 \pmod 2$ so put $x = 1 + 2t_1$. Substitute in $x \equiv 2 \pmod 3$ gives:

$$1 + 2t_1 \equiv 2 \,(\text{mod } 3) \Rightarrow 2t_1 \equiv 1 \,(\text{mod } 3) \Rightarrow 2t_1 \equiv 4 \,(\text{mod } 3)$$

$$t_1 \equiv 2 \,(\text{mod } 3) \Rightarrow t_1 = 2 + 3t_2.$$

Hence $x = 1 + 2t_1 = 1 + 2(2 + 3t_2) = 5 + 6t_2$. Substituting in $x \equiv 3 (\text{mod } 5)$ gives:

$$5 + 6t_2 \equiv 3 \,(\text{mod } 5) \Rightarrow 6t_2 \equiv -2 \equiv 3 \,(\text{mod } 5)$$

$$\Rightarrow 2t_2 \equiv 1 \,(\text{mod } 5) \Rightarrow 2t_2 \equiv 6 \Rightarrow t_2 \equiv 3 \,(\text{mod } 5)$$

$$\Rightarrow t_2 = 3 + 5t.$$

Hence $x = 5 + 6(3 + 5t) = 23 + 30t$. In particular, the smallest positive solution is $x = 23$.

Comment In general the *Chinese Remainder Theorem* says that the system of k congruences $x \equiv a_i \,(\text{mod } m_i)$where each pair of moduli is relatively prime has a unique least residue solution modulo $m_1 m_2 \cdots m_k$. The substitution technique above can be applied to find that solution.

7. We have $n = 2t_1 + 1$ and

$$2t_1 + 1 \equiv 0 \,(\text{mod}\, 3) \Rightarrow 2t_1 \equiv 2 \;(\text{mod}\, 3) \Rightarrow t_1 = 3t_2 + 1$$

$$\Rightarrow n = 2(3t_2 + 1) + 1 = 6t_2 + 3.$$

$$6t_2 + 3 + 2 \equiv 0 \pmod 5 \Rightarrow t_2 = 5t_3 \Rightarrow n = 30t_3 + 3.$$

$$30t_3 + 3 + 4 \equiv 0 \pmod 7 \Rightarrow t_3 \equiv 7t_4$$

$$\Rightarrow n = 210t_3 + 3.$$

We conclude that the least $n > 3$ that satisfies all constraints is $n = 210 + 3 = 213$.

8. We have that the equations imply that

$$x + 2y \equiv 3 \text{ (mod 7)}$$

$$\Rightarrow 5x \equiv 1 \text{ (mod 7)} \Rightarrow 5x \equiv 15 \text{ (mod 7)} \Rightarrow x \equiv 3 \text{ (mod 7)}$$

$$\Rightarrow 2y \equiv 0 \pmod 7 \Rightarrow y \equiv 0 \text{ (mod 7)}.$$

Hence the least residue solutions modulo 7 are $x = 3$, $y = 0$.

9. Consider $ax \equiv b$ (mod 20) and let $d = (a, 20)$ (the gcd of a and 20). If d does not divide b (which is possible for example if $d = 2$ and $b = 3$)), then there are no solutions. Otherwise there are d solutions. The set of possible values of d is the set of divisors of 20, which is $\{1, 2, 4, 5, 10, 20\}$, and each such d is attainable by taking $a = b = d$ in the equation. The set has 6 members so there are $6 + 1 = 7$ different possibilities for the number of least residue solutions to such a congruence, these being $0, 1, 2, 4, 5, 10$ and 20.

10. Five Thursdays in February occurs exactly when we have a leap year with February 29th being a Thursday, which happened in 1968. Starting our count of the week from Thursday we may write this event as $x = 0$, where x is the value of the weekday on February 29th. The next occurence of February 29th is $4 \times 365 + 1$ days later. Now

$$4 \times 365 + 1 \equiv 4 \times 1 + 1 = 5 \text{ (mod 7)}.$$

Hence the value of x is incremented by 5 each leap year cycle. Let us find the least number t of cycles before $x = 0$ again, which is to say that $5t \equiv 0$ (mod 7) which implies $t = 7$, so day-of-the-week coincidences happen once every $7 \times 4 = 28$ years. Now $2100 - 1968 = 132$ and $\frac{132}{28} = 4\frac{20}{28}$. Hence the cycle will be completed on only four subsequent occasions between 1968 and 2100, those being

$$1968 + 28 = 1996,\ 1996 + 28 = 2024,\ 2024 + 28 = 2052,\ 2052 + 28 = 2080.$$

Problem Set 2

1. Working modulo 2 we get that $y = 2t$ say, so we have

$$2x + 2t = 2 \Rightarrow x = 1 - t;$$

hence the solutions set is

$$\{(x,y) : x = 1-t,\, y = 2t,\, t \in \mathbb{Z}\}.$$

2. Working mod 15 we get $y \equiv 2 \pmod{15}$ so we put $y = 15t + 2$ and we obtain

$$15x + 16(15t+2) = 17 \Rightarrow 15x = -16(15t) - 15$$
$$\Rightarrow x = -16t - 1,$$

hence, by replacing t by $-t$, which is legal as t can be any integer, the solution set is

$$\{(x,y) : x = 16t - 1,\, y = 2 - 15t,\, t \in \mathbb{Z}\}.$$

3. Again working mod 15 we get $3y \equiv 2 \pmod{15}$ and since $d = (3,15) = 3$ is not a factor of 2, there are no solutions.

4. Working modulo 7 we have $y \equiv 2 \pmod 7$ so we put $y = 2 + 7t$. Substituting accordingly we obtain

$$7x + 15(2+7t) = 51 \Rightarrow 7x = 7(-15t) + 21$$
$$\Rightarrow x = 3 - 15t.$$

We also require

$$2 + 7t \geq 1 \Rightarrow t \geq -\frac{1}{7} \Rightarrow t \geq 0;$$
$$3 - 15t \geq 1 \Rightarrow t \leq \frac{2}{15} \Rightarrow t \leq 0.$$

Hence the solution set is unique: $x = 3$,$y = 2$.

5. We have

$$6x - 15y = 51 \Leftrightarrow 2x - 5y = 17.$$

Working modulo 2 gives $-y \equiv 1 \pmod 2$ which implies $y = 1 + 2t$. Substituting accordingly gives

$$2x - 5(1+2t) = 17 \Rightarrow 2x = 10t + 22 \Rightarrow x = 5t + 11.$$

However we also require

$$y = 1 + 2t \leq -1 \Rightarrow 2t \leq -2 \Rightarrow t \leq -1;$$
$$x = 5t + 11 \leq -1 \Rightarrow 5t \leq -12 \Rightarrow t \leq -\frac{12}{5} \Rightarrow t \leq -3.$$

Hence the solution set is

$$\{(x,y) : x = 5t + 11,\, y = 1 + 2t,\, t \leq -3\}.$$

However,

$$t \leq -3 \Leftrightarrow -t \geq 3 \Leftrightarrow -t - 3 \geq 0,$$

so putting $s = -t - 3$ so that $t = -s - 3$ we get the formulation: $x = 5t + 11 = 5(-3 - s) + 11 = -4 - 5s$ and $y = 1 + 2t = 1 + 2(-3 - s) = -5 - 2s$, giving as solution set

$$\{(x, y) : x = -4 - 5s,\ y = -5 - 2s,\ s \geq 0\}.$$

6. Subtracting the first equation from the second eliminates x and gives $y + 2z = 10$ so that $y = 2t$ is even. Then $2z = 10 - 2t \Rightarrow z = 5 - t$. We then have

$$x + y + z = x + 2t + (5 - t) = x + t + 5 = 31 \Rightarrow x = 26 - t.$$

Hence we require

$$26 - t \geq 1 \Rightarrow t \leq 25,\ 2t > 0 \Rightarrow t \geq 1\, 5 - t \geq 1 \Rightarrow t \leq 4;$$

$$\Rightarrow 1 \leq t \leq 4.$$

This gives four solutions triples for (x, y, z)

$$\{(25, 2, 4), (24, 4, 3), (23, 6, 2), (22, 8, 1)\}.$$

7. With a natural use of symbols we have the simultaneous equations:

$$c + s + w = 35,\ 100c + 8s = 296.$$

Multiplying the first by 8 and subtracting from the second we get

$$92c - 8w = 16 \Rightarrow 23s - 2w = 4.$$

Modulo 2 we have s is even: $s = 2t$. Hence $46t - 2w = 4$ so that $w = 23t - 2$. Finally

$$c = 35 - s - w = 35 - 2t - 23t + 2 = 37 - 25t.$$

Assuming there is at least one of each type of creature we have

$$s \geq 1 \Leftrightarrow 2t \geq 1 \Leftrightarrow t \geq \frac{1}{2} \Leftrightarrow t \geq 1;$$

$$w \geq 1 \Leftrightarrow 23t - 2 \geq 1 \Leftrightarrow t \geq \frac{3}{23} \Leftrightarrow t \geq 1;$$

$$c \geq 1 \Leftrightarrow 37 - 25t \geq 1 \Leftrightarrow t \leq \frac{36}{25} \Leftrightarrow t \leq 1.$$

Hence $t = 1$ and we get $(c, s, w) = (12, 2, 21)$. In particular there are 21 worms.

8. A farmer sold her sheep for £180 each and her cows for £290 a piece, receiving £2890. How many cows did she sell?

As a diophantine equation we have, upon dividing by 10,

$$18s + 29c = 289;$$

modulo 18 we have $11c \equiv 1 \pmod{18} \Rightarrow 11c \equiv 55 \pmod{18}$ so that $c \equiv 5 \pmod{18}$. Putting $c = 5$ we get

$$s = \frac{289 - (29)5}{18} = \frac{144}{18} = 8,$$

and $(c, s) = (5, 8)$ is a feasible solution pair. Testing $c = 5 + 18 = 23$ or any greater value will give a negative value for s, so this is the only solution, and so the farmer sold 5 cows.

9. Let a and m be the current ages of Anne and Mary respectively. Let t be the time in the future when the comparison in the first sentence is made. Then we have

$$a + t = \frac{1}{2}(3m) \Rightarrow t = \frac{3}{2}m - a.$$

And the second part of the sentence translates as

$$m + t = 5a \Rightarrow m + (\frac{3}{2}m - a) = 5a \Rightarrow \frac{5}{2}m = 6a$$

$$\therefore m = \frac{12a}{5}.$$

Hence a is a multiple of 5. Putting $a = 5$ gives $m = 12$. Putting $a = 10$ gives $m = 24$ and then Mary could vote. Hence Anne is 5. (Unless both Anne and Mary are 0.)

10. Let a and b be numbers of records that Andy and and Bob sold at the full price of £5. Letting p stand for the unknown lower price we have the equation

$$5a + (30 - a)p = 5b + (40 - b)p \qquad (1)$$

$$\Rightarrow (30 - a - 40 + b)p = 5(b - a) \Rightarrow (b - a - 10)p = 5(b - a)$$

$$(10 + c)p - 5c = 0, \text{ where } c = a - b$$

$$c(p - 5) = -10p \Rightarrow c = \frac{10p}{5 - p}.$$

The only integer values of p with $1 \leq p \leq 4$ that give integer values for c are $p = 3$ ($c = 15$) and $p = 4$ ($c = 40$). For $p = 4$ however we have $a - b = 40$ so that $a = 40 + b$, which is not possible as Andy only had 30 records to sell. For $p = 3$ we have $a = 15 + b$. The common sum received is $2a + 90 = 2b + 120$. Since $b \geq 0$ the least they could have got is £120.

Problem Set 3

1. The positive integers $k \leq p^m$ that are *not* relatively prime to p^m are $p, 2p, 3p, \cdots p^{m-1}p$ and so $\phi(p^m) = p^m - p^{m-1} = p^{m-1}(p - 1)$.

2. Let the prime decomposition of k be $k = p_1^t \cdots p_r^{t_r}$. Then by Question 1 we have

$$\phi(k) = \phi(p_1^{t_1}) \cdots \phi(p_r^{t_r}) = \Pi_{i=1}^r p^{t_i - 1}(p_i - 1)$$

$$= \Pi_{i=1}^r p_i^{t_i}(1 - \frac{1}{p_i}) = k\Pi_{i=1}^r(1 - \frac{1}{p_i}).$$

Comment This formula shows that $\phi(n)$ can be calculated just from knowledge of the set of prime divisors of k. The full prime decomposition is not required.

3. $n = pq = 3 \times 11 = 33$. $\phi(n) = (p-1)(q-1) = 2 \times 10 = 20$. Since $e = 7$ is not a factor of 20, e satisfies the given criterion.

4. We need to solve $7d \equiv 1 \pmod{20}$ so that $7d \equiv 21 \pmod{20}$ whence $d \equiv 3 \pmod{20}$ so $d = 3$ is the required least residue solution.

5. $6^2 = 36 \equiv 3 \pmod{33}$; $6^4 \equiv 3^2 \equiv 9 \pmod{33}$ so that

$$M^e = 6^7 = 6^4 \times 6^2 \times 6 \equiv 3 \times 9 \times 6 \equiv 27 \times 6 \equiv (-6) \times 6$$

$$\equiv -36 \equiv -3 \equiv 30 \,(\text{mod}\, 33).$$

Hence Bob's transmission is 30.

6. Since $ed \equiv 1 \pmod{\phi(n)}$ we may write $ed = 1 + k\phi(n)$ for some integer k. Then

$$M^{ed} \equiv M^{1+k\phi(n)} \equiv M \cdot (M^{\phi(n)})^k \equiv M \cdot 1^k \equiv M \,(\text{mod}\, n).$$

7. In this case $M^e \equiv 30 \pmod{33}$ so that

$$M = M^{ed} = 30^3 \equiv (-3)^3 = -27 \equiv 6 \,(\text{mod}\ 33).$$

Hence Alices recovers Bob's plaintext message $M = 6$.

8. We have $n = pq = 23 \times 47 = 1081$ and $e = 15$ is given. Bob transmits $77^{15} \pmod{1081}$. Now $77^2 = 5929 = 5 \times 108a + 524 \equiv 524 \pmod{1081}$; $77^4 \equiv 524^2 = 274,576 = 254 \times 1081 + 2 \equiv 2 \pmod{1081}$; $77^8 \equiv 2^2 = 4$ (mod 1081). Hence

$$77^{15} = 77^8 \times 77^4 \times 77^2 \times 77 \equiv 4 \times 2 \times 524 \times 77 = 616 \times 524 = 308 \times 1048$$

$$\equiv 308 \times (-33) = 924 \times (-11) = (-157) \times (-11) = 1727 \equiv 646 \,(\text{mod}\, 1081).$$

Hence Bob's transmission is 646.

9. First, $\phi(n) = (p-1)(q-1) = 22 \times 46 = 1012$. We solve $ed \equiv 1 \pmod{\phi(n)}$, which is $15d \equiv 1 \pmod{1012}$. We note for the information in our calculation that $1012 = 4 \times 11 \times 23$.

$$15d \equiv 2025 \pmod{1012} \Rightarrow 3d \equiv 405 \pmod{1012} \Rightarrow d \equiv 135 \pmod{1012}.$$

And so the final ingredient in Alice's private key is $d = 135$.

10. Alice needs to calculate $M^{ed} \pmod{n}$, which is to say $646^{135} \pmod{1081}$. Working modulo 1081 throughout we get $646^2 = 417316 = 386 \times 1081 + 50 \equiv 50$;

$$646^4 \equiv 50^2 = 2500 = 2 \times 1081 + 338 \equiv 338;$$

$$646^8 = (646^4)^2 \equiv 338^2 = 114244 = 105 \times 1081 + 739 \equiv 739;$$

$$646^{16} = (646^8)^2 \equiv 739^2 = 546121 = 505 \times 1081 + 216 \equiv 216;$$

$$646^{128} = (646^{16})^8 \equiv 216^8 = 6^{24} = (6^4)^6 = 1296^6 \equiv 215^6 = (46225)^3$$

$$\equiv (42 \times 1081 + 823)^3 \equiv (-253)^3 = -17173512$$

$$= 15886 \times 1081 - 746 \equiv 335.$$

$$\text{Hence } 646^{135} = 646^{128} \times 646^4 \times 646^2 \times 646 \equiv 335 \times 338 \times 50 \times 646$$

$$\equiv 113230 \times 32300 \equiv (104 \times 1081 + 806)(29 \times 1081 + 951)$$

$$\equiv 806 \times 951 \equiv (-275)(-130) = 35750 = 33 \times 1081 + 77 \equiv 77;$$

therefore Alice recovers Bob's plaintext message as $M = 77$.

Problem Set 4

1. Since $A \neq 0 \pmod{p}$ we can multiply through by A' where $AA' \equiv 1 \pmod{p}$ to get an equivalent equation $x^2 + A'Bx + C \equiv 0 \pmod{p}$. If $A'B$ is even we may now complete the square:

$$\left(x + \frac{A'B}{2}\right)^2 \equiv \left(\frac{A'B}{2}\right)^2 - C \pmod{p}$$

to get an equation of the form $y^2 \equiv a \pmod{p}$. On the other hand, if $A'B$ is odd, then $A'B \equiv A'B + p \pmod{p}$ and the latter is even and we can proceed in the same way to get:

$$\left(x + \frac{A'B + p}{2}\right)^2 \equiv \left(\frac{A'B + p}{2}\right)^2 - C \pmod{p}.$$

2. First we solve $2a \equiv 1 \pmod{7}$, which gives $a \equiv 4 \pmod{7}$. Hence, multiplying through by 4 and working modulo 7 we have

$$2x^2 + 3x + 1 \equiv x^2 + 5x + 4 \equiv x^2 - 2x + 4 \equiv 0 \pmod{7}$$

$$\Rightarrow (x - 1)^2 \equiv -4 + 1 \equiv 4 \pmod{7}.$$

$$\Rightarrow x - 1 \equiv \pm 2 \Rightarrow x \equiv 3 \text{ or } -1.$$

Hence the least residue solutions are 3 and 6.

3. First we solve $3a \equiv 1 \pmod{7}$, which is $3a \equiv 15 \pmod{7}$ so that $a \equiv 5 \pmod{7}$. Hence, multiplying $3x^2 + x + 4$ by 5 we have modulo 7:

$$x^2 - 2x - 1 \equiv 0 \Rightarrow (x - 1)^2 \equiv 1 + 1 \equiv 2 \pmod{7}$$

$$\Rightarrow x - 1 \equiv 3 \text{ or } 4 \pmod{7} \Rightarrow x \equiv 4 \text{ or } 5 \pmod{7}.$$

Hence the solutions are 4 and 5.

4. Given that $r^2 \equiv a \pmod{p}$ it follows that $p - r$ is also a solution as $(p - r)^2 = p^2 - 2pr + r^2 \equiv r^2 \equiv a \pmod{p}$. Moreover $p - r$ is a new solution for if $r \equiv p - r \pmod{p}$ then $2r \equiv p \equiv 0 \pmod{p}$ and so $r \equiv 0 \pmod{p}$, which is not the case as $a \not\equiv 0 \pmod{p}$.

Next suppose that $s^2 \equiv 0 \pmod p$ for some least residue s. Then $r^2 - s^2 = (r-s)(r+s) \equiv 0 \pmod p$ so that p is a factor of $r-s$ or $r+s$. Since $r-s$ are least residues it follows that either $r-s=0$ so that $s=r$ or $r+s=p$ so that $s=p-r$. Hence there are either no solutions or exactly two least residue solutions to $x^2 \equiv a \pmod p$.

5. For a prime p we have $\phi(p) = p-1$ so that if p is not a factor of a then $a^{\phi(p)} \equiv 1 \pmod p$ becomes $a^{p-1} \equiv 1 \pmod p$ so that $a^p \equiv a \pmod p$. On the other hand, if $a \equiv 0 \pmod p$ then $a^P \equiv 0 \pmod p$ also so that, in any event, $a^p \equiv a \pmod p$.

6. Since p is odd, $\frac{p-1}{2}$ is integral. Let $a^{\frac{p-1}{2}} = r$. Then by Question 5

$$r^2 = \left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1 \pmod p$$

so $r = \pm 1 \pmod p$.

7. Here $\frac{p-1}{2} = \frac{31-1}{2} = 15$ and $a = 7$. Now working mod 31 we have

$$7^2 = 49 \equiv 18,\ 7^4 \equiv 18^2 \equiv 324 \equiv 14,\ 7^8 \equiv 14^2 = 196 \equiv 10 \pmod{31}$$
$$\Rightarrow 7^{16} \equiv 10^2 \equiv 100 \equiv 7 \pmod{31}$$
$$\Rightarrow 7^{15} \equiv 1 \pmod{31}$$

and so, by the Euler criterion, 7 is a quadratic residue mod 31.

8.
$$x^2 \equiv 7 \equiv 38 \equiv 69 \equiv 100 = 10^2 \pmod{31}$$
$$\Rightarrow x \equiv \pm 10 \pmod{31},$$

so $x = 10$ or $x = 21$.

9.
$$x^2 \equiv 41 \equiv 102 \equiv 163 \equiv 224 = 4^2 \times 14 \pmod{61}$$
$$\Rightarrow \left(\frac{x}{4}\right)^2 \equiv 14 \equiv 75 = 5^2 \times 3 \pmod{61}$$
$$\Rightarrow \left(\frac{x}{4 \times 5}\right)^2 \equiv 3 \equiv 64 = 8^2 \pmod{61}$$
$$\Rightarrow x^2 \equiv 4^2 \times 5^2 \times 8^2 \pmod{61}$$
$$\Rightarrow x \equiv \pm 4 \times 5 \times 8 = \pm 160 = \pm 38 \pmod{61},$$

so that $x = 38$ or $x = 61 - 38 = 23$.

10. The equation $ab \equiv r \pmod p$ implies that

$$(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \pmod p \tag{2}$$

and since a is a quadratic residue this is equivalent to

$$b^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \pmod p,$$

and so for b to be a quadratic residue, r must be a quadratic residue. Conversely, if r is a quadratic residue then so is ab and then, since $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, the same must be true of b. Therefore b will be a quadratic residue if and only if r is a quadratic residue.

Problem Set 5

1. If one of the equations $x^2 \equiv a \pmod p$, $x^2 \equiv b \pmod p$ has a solution then so does the other (the same solution) as $a \equiv b \pmod p$.

2. Let r be the least residue of $a \pmod p$. Then $x^2 \equiv r^2 \pmod p$ has the two solutions $x = \pm r$ and since $a^2 \equiv r^2$ these are also solutions to $x^2 \equiv a^2 \pmod p$. Therefore $(a^2/p) = 1$.

3. Since $(a/p) = 1$ if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ it follows that $(a/p) \equiv a^{\frac{p-1}{2}} \pmod p$. Hence

$$(ab/p) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (a/p)(b/p) \pmod p.$$

Now we need only note that both sides of this congruence are equal to ± 1 and since p is an odd prime, $1 \equiv -1 \pmod p$ is impossible. Therefore we conclude that $(ab/p) = (a/p)(b/p)$.

4. By Question 1 and then 2 we have $(19/5) = (4/5) = 1$; $(-9/13) = (4/13) = (2^2/13) = 1$.

5. We want $(85/97) = (5 \times 17/97) = (5/97)(17/97)$. Now, since $5 \equiv 1 \pmod 4$ by the QRT

$$(5/97) = (97/5) = (2/5) = -1$$

the last equality be found by inspecting cases or using the given rule for $(2/p)$. On the other hand, again by the QRT

$$(17/97) = (97/17) = (12/17) = (3/17)(4/17) = (17/3) \times 1$$

$$= (2/3) = -1;$$

hence $(85/97) = (-1)(-1)$ and so the congruence has solutions.

Comment Another calculation route uses the result of Question 6:

$$(85/97) = (-12/97) = (-1/97)(3/97)(4/97) = (-1/97)(97/3) \times 1$$

$$= (-1/97)(1/3) = (-1/97) \times 1 = 1$$

since $97 \equiv 1 \pmod 4$.

6. By Euler's criterion $(-1/p) \equiv (-1)^{\frac{p-1}{2}} \pmod 4$. Hence $(-1/p) = 1$ if and only if $\frac{p-1}{2} = 2k$ say, whence $p = 4k+1$, which is to say if and only if $p \equiv 1 \pmod 4$.

7.

$$(3201/8191) = (3/8191)(11/8191)(97/8191);$$

but since $8191 \equiv 3 \pmod 4$ we have by the QRT:

$$(3/8191) = -(8191/3) = -(1/3) = -1;$$

$$(11/8191) = -(8191/11) = -(7/11) = -(-(11/7)) = (4/7) = 1;$$

$$(97/8191) = (8191/97) = (43/97) = (97/43) = (11/43)$$

$$= -(43/11) = -(-1/11) = -(-1) = 1.$$

$$\therefore (3201/8191) = (-1)(1)(1) = -1.$$

Hence there is no solution to the quadratic congruence $x^2 \equiv 3210 \pmod{8191}$.

8.

$$(14/31) = (2/31)(7/31) = (-1)(-(31/7) = (4/7) = 1.$$

$$x^2 \equiv 14 \equiv 45 = 3^2 \times 5 \pmod{31}$$

$$\Rightarrow (\frac{x}{3})^2 \equiv 5 \equiv 36 = 6^2 \pmod{31}$$

$$\Rightarrow \frac{x}{3} = \pm 6 \pmod{31} \Rightarrow x \equiv \pm 18 \pmod{31}$$

so that the solutions are 13 and 18.

9.

$$(p/q) = (q + 4a/q) = (4a/q) = (4/q)(a/q) = (a/q)$$

$$(q/p) = (p - 4a/p) = (-4a/p) = (4/p)(-1/p)(a/p) = (-1/p)(a/p).$$

Now if $p \equiv q \equiv 3 \pmod 4$ then $(-1/p) = -1$ and by the CRT

$$(a/q) = (p/q) = -(q/p) = -(-1)(a/p)$$

so that $(a/p) = (a/q)$ in this case. Since $p \equiv q \pmod 4$ the only other case is when $p \equiv q \equiv 1 \pmod 4$ then

$$(a/q) = (p/q) = (q/p) = (1)(a/p)$$

and so again $(a/p) = (a/q)$. In both cases then $(a/p) = (q/p)$.

10. Here $159 = 3 \times 53$. We wish to solve $x^2 \equiv 211 \equiv 52 \pmod{159}$. Since $159 = 3 \times 53$, we have $x^2 \equiv 52 \pmod 3$ and $x^2 \equiv 52 \pmod{53}$. Taking the first of these congruences:

$$x^2 \equiv 1 \pmod 3 \Rightarrow x \equiv 1, 2 \pmod 3.$$

Putting $x = 3t + 1$ and substitute into $x^2 \equiv -1 \pmod{53}$ so that modulo 53 we have

$$(1 + 3t)^2 \equiv -1 \Rightarrow 9t^2 + 6t + 2 \equiv 0;$$

$9a \equiv 1 \pmod{53}$ implies the multiplier $a = 6$ so

$$t^2 + 36t + 12 = (t + 18)^2 \equiv -12 + 324 = 312 \equiv -6 \pmod{53}$$

$$\Rightarrow (t + 18)^2 \equiv 100 \pmod{53}$$

$$\Rightarrow t + 18 = 10 \,\text{or}\, 43 \Rightarrow t = 25 \,\text{or}\, 45$$

$$\Rightarrow x = 3t + 1 = 76 \,\text{or}\, 136.$$

Alternatively, we put $x = 3t + 2$, we have modulo 53

$$(2 + 3t)^2 \equiv -1 \Rightarrow 9t^2 + 12t + 5 \equiv 0;$$

$$\Rightarrow t^2 + 72t + 30 \equiv 0$$

$$\Rightarrow (t + 36)^2 \equiv 1266 \equiv -6 \equiv 10^2 \pmod{53}$$

$$\Rightarrow t + 36 = 10 \text{ or } 43 \,(\text{mod } 53)$$

$$\Rightarrow t = 7 \text{ or } 27$$

$$\Rightarrow x = 23 \text{ or } 83.$$

Hence the full set of solutions is $\{23, 76, 83, 136\}$.

Problem Set 6

1. Suppose to the contrary that $(0, \frac{1}{2})$ were countable so there exists a bijection $f : \mathbb{N} \to (0, \frac{1}{2})$. Then $2f : \mathbb{N} \to (0, 1)$ is a bijection, which gives the contradiction that $(0, 1)$ is countable. It follows therefore that $(0, \frac{1}{2})$ is an uncountable set.

2. Since each A_i is countable, the members of A_i may be listed as

$$a_{1,i}, a_{2,i}, \cdots, a_{j,i}, \cdots.$$

Let $B_m = \{a_{i,j} : i + j = m\}$, $m = 2, 3, \cdots$. Now each B_m is finite and indeed we may list the members of B_m as $a_{1,m-1}, a_{2,m-2}, \cdots, a_{m-1,1}$. We can define a list of the set $B = \bigcup_{m=2}^{\infty} B_m$ by listing all the members of B_2 then of B_3, and so on. This shows that B is a countable set but clearly $B = A$ so that A, the union of countably many countable sets, is itself countable.

3. Since $\mathbb{Z} \subseteq \mathbb{Q}$ and a subset of a countable set is countable, it is enough to prove that $\mathbb{Q}$ is countable. After the fashion of Question 2, let $B_m = \{\frac{p}{q} \in \mathbb{Q}^+ : p + q = m\}$ $(m \geq 2)$. Again since each B_m is finite and the union of all the B_m is a countable union of countable sets, it follows that $\mathbb{Q}$ is countable. Since the mapping $x \to -x$ defines a bijection from the positive to the negatives rationals, it follows that the latter set, $\mathbb{Q}^-$ is also countable. Finally then $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$ is the union of three countable sets, and so $\mathbb{Q}$ is countable.

4. Suppose to the contrary that I was countable. Then by Question 3, $\mathbb{Q}$ is a countable set and so $\mathbb{R} = \mathbb{Q} \cup I$ would be countable, it being the union of two countable set. However then $(0, 1)$, being a subset of a countable set, would also be countable. This is a contradiction so we conclude that I is not a countable set.

5. It is enough to prove the result for $n = 2$ for given this there is an obvious bijection between $A = A_1 \times A_2 \times \cdots \times A_n$ and $(A_1 \times A_2 \times \cdots \times A_{n-1}) \times A_n$ and by induction and the $n = 2$ case, it follows that A is countable. Since A_1 and A_2 are countable their members can be listed as $a_1, a_2, \cdots$ and $b_1, b_2, \cdots$ respectively. We can then write $A_1 \times A_2$ as the countable union of finite sets B_m where $B_m = \{(a_i, b_j) : i + j = m\}$ $m = 2, 3, \cdots$.

6. The members of the infinite product $P = A \times A \times A \times \cdots$ consist of all infinite binary strings. There is then a bijection from P into $[0, 1)$ by which the binary string $(\varepsilon_1, \varepsilon_2, \cdots)$ is mapped to $0 \cdot \varepsilon_1\varepsilon_2 \cdots$ taken as a binary expansion of the correpsonding real number. However $[0, 1)$ contains the uncountable set $(0, 1)$ and so $[0, 1)$ and therefore P also, is uncountable.

7. For each $b \in f(A)$, choose $a \in A$ such that $f(a) = b$. The mapping $g : B \to A$ by which $b \mapsto a$ is then a one-to-one function from B into A. If B were uncountable, then so would be its bijective imaged, $g(B) \subseteq A$ so that the containing set A would be uncountable as well. This contradicts the give hypothesis that A is countable, so we conclude that the range of a function from a countable set is itself a countable set.

8. Yes. Since $B \cap C$ is a subset of the countable set C, it follows that $B \cap C$ is countable. Then $A \cup (B \cap C)$ is the union of two countable sets, and so by the result of Question 2, $A \cup (B \cap C)$ is countable.

9.The direct product of two uncountable sets A, B is uncountable, for if $A \times B$ were countable, so would be the subset $S = \{(a, b) : a \in A\}$ where $b \in B$ is a fixed member of B. However the projection mapping $(a, b) \mapsto a$ is a bijection from S onto A, and this would give the contradiction that A were countable. (In fact this argument shows that the direct product of an uncountable set and a non-empty set is uncountable.) In particular, since $\mathbb{R}$ is uncountable (as it contains the uncountable open interval $(0, 1)$), it follows that $\mathbb{R} \times \mathbb{R}$ is uncountable. Now observe that the mapping whereby $a + bi \mapsto (a, b)$ is a bijection from $\mathbb{C}$ onto $\mathbb{R} \times \mathbb{R}$, and so both sets are uncountable.

10. Let P_n denote the set of polynomials with rational coefficients of degree at most n. Then the mapping whereby $a_0 + a_1x + \cdots + a_nx^n \mapsto (a_0, a_1, \cdots, a_n)$ is a bijection from P_n into the n-fold direct product $\mathbb{Q} \times \mathbb{Q} \times \cdots \times \mathbb{Q}$ of the rationals. By Question 5, it follows that P_n is countable. Now each $p(x) \in P_n$ has at most n roots. Hence the set of all real numbers that are roots of polynomials in P_n can be listed by listing all members of P_n as $p_1, p_2, \cdots$ and forming a list of their roots by listing all the roots of p_1, then of p_2, and so on. It follows that the set of real numbers R_n that are roots of polynomials in P_n is countable. Finally, the set A of all agebraic numbers is the union $A = \bigcup_{n=1}^{\infty} R_n$ and so A is countable by Question 2, A is a countable union of countable sets.

Finally, by definition, $\mathbb{R}$ is the (disjoint) union of A and T, the set of all transcendental (ie non-algebraic) numbers. If T were countable, then $\mathbb{R} = A \cup T$, being the union of two countable sets, would be countable. We know this is not the case so it follows that T is an uncountable set.

Comment We have thus shown that the set of transcendental numbers is uncountable without identifying a single one of them! The result has been proved just through comparing various sets with one another and seeing whether they can or cannot be put into one-to-one correspondence. The transcendentals is an obscure club - the famous numbers e and π are members but this is a fact that either openly reveals!

Problem Set 7

1. By inspection of the first few values of u_n we may try to prove inductively that $u_n = 2^n - 1$. Certainly this gives $u_0 = 0$ so let us assume that the formula holds for some value of $n \geq 0$ and examine u_{n+1}. We get

$$u_{n+1} = 2u_n + 1 = 2(2^n - 1) + 1 = 2^{n+1} - 2 + 1 = 2^{n+1} - 1,$$

and so the validity of the solution is established by induction.

2. Put $u_n = Aw^n$ into the give recurrence relation we get

$$Aw^{n+1} = Aw^n + Aw^{n-1} \Rightarrow w^2 - w - 1 = 0;$$

solving we get $w = \frac{1 \pm \sqrt{5}}{2}$. It follows that $u_n = A_1 w_1^n + A_2 w_2^n$, where $w_1 = \frac{1+\sqrt{5}}{2}$ and $w_2 = \frac{1-\sqrt{5}}{2}$ satisfies the Fibonacci recurrence. Putting $u_0 = 0$ and $u_1 = 1$ then gives the equations:

$$A_1 + A_2 = 0, \ A_1 w_1 + A_2 w_2 = 1;$$

putting $A_2 = -A_1 = -A$ say we then have:

$$A(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}) = 1 \Rightarrow A = \frac{1}{\sqrt{5}} \text{ and so}$$

$$f_n = \frac{1}{\sqrt{5}}\big[\big(\frac{1+\sqrt{5}}{2}\big)^n - \big(\frac{1-\sqrt{5}}{2}\big)^n\big], \ n = 0, 1, 2, \cdots.$$

3.

$$\lim_{n\to\infty} \frac{f_{n+1}}{f_n} = \lim_{n\to\infty} \frac{w_1^{n+1} - w_2^{n+1}}{w_1^n - w_2^n},$$

since $||w_2| < 1$ and $|w_1| > 1$ it follows that this limit is $w_1 = \frac{1+\sqrt{5}}{2}$, so that the Fibonacci sequence is asymptotically a geometric sequence with common ratio equal to the golden ratio.

4. The given substitution yields the equation

$$pAw^{n+1} - Aw^n + qAw^{n-1} = 0 \Rightarrow pw^2 - (p+q)w + q = 0,$$

$$\Rightarrow (w-1)(pw-q) = 0 \Rightarrow w_1 = 1, \ w_2 = \frac{q}{p}$$

so candidate solutions are $u_n = A_1(1)^n = A_1$ and $u_n = A_2\big(\frac{q}{p}\big)^n$, $n = 0, 1, 2, \cdots$.

5. Put $u_n = A_1 + A_2(\frac{q}{p})^n$ into $pu_{n+1} - u_n + qu_{n-1}$to obtain:

$$[pA_1 + pA_2(\frac{q}{p})^{n+1}] - [A_1 + A_2(\frac{q}{p})^n] + [qA_1 + qA_2(\frac{q}{p})^{n-1}]$$

$$= A_1(p-1+q) + A_2(\frac{q}{p})^{n-1}[p(\frac{q}{p})^2 - \frac{q}{p} + q],$$

which, since $p + q = 1$ simplifies to

$$A_2(\frac{q}{p})^{n-1}[\frac{q^2}{p} - \frac{q}{p} + q] = 0$$

as required because the inside bracket equals

$$\frac{q^2 - q + pq}{p} = \frac{q(q-1) + pq}{p} = \frac{-pq + pq}{p} = 0.$$

6. From our general solution $u_n = A_1 + A_2(\frac{q}{p})^n$ we put $u_0 = 0$ to get $A_1 + A_2 = 0$, so that we may write $A_2 = -A_1$. Next putting $u_l = 1$ gives,

$$A_1 - A_1(\frac{q}{p})^l = 1 \Rightarrow A_1 = \frac{1}{1 - (\frac{q}{p})^l}, \; A_2 = \frac{1}{(\frac{q}{p})^l - 1}, \text{ hence}$$

$$u_n = \frac{1}{1 - (\frac{q}{p})^l} + \frac{(\frac{q}{p})^n}{(\frac{q}{p})^l - 1} = \frac{(\frac{q}{p})^n - 1}{(\frac{q}{p})^l - 1}, \; n = 0, 1, 2, \cdots.$$

7. We seek a solution of the form $u_n = A_1 + A_2 n$, which we verify does satisfy the recurrence:

$$\frac{u_{n+1} + u_{n-1}}{2} = \frac{A_1 + (n+1)A_2 + A_1 + (n-1)A_2}{2}$$

$$= \frac{2A_1 + 2nA_2}{2} = A_1 + A_2 n = u_n, \text{ as required.}$$

Putting $u_0 = 0$ gives $A_1 = 0$ and then $u_l = 1$ gives $A_2 l = 1$ so that $A_2 = \frac{1}{l}$, our required solution is thus $u_n = \frac{n}{l}$.

8. From Question 5 we have that the suggested augmented solution has the form

$$v_n = A_1 + A_2(\frac{q}{p})^n + kn.$$

We require that $pv_{n+1} - v_n + qv_{n-1}$ return the value -1 so that k must satisfy:

$$pk(n+1) - kn + qk(n-1) = -1 \text{ so that}$$

$$pkn + pk - kn + qkn - qk = -1 \Rightarrow (p + q - 1)kn + (p - q)k = -1$$

and since $p+q=1$ we conclude that

$$k = \frac{1}{q-p}.$$

Giving the general solution:

$$v_n = A_1 + A_2\big(\frac{q}{p}\big)^n + \frac{n}{q-p}.$$

9. The suggested candidate for solution has the form $v_n = A_1 + A_2 n + kn^2$. Hence we require that substituion of $v_n = kn^2$ into the expression $pv_{n+1} - v_n + qv_{n-1}$ yields -1, which is to say:

$$\frac{k(n+1)^2}{2} - kn^2 + \frac{k(n-1)^2}{2} = -1$$
$$\Rightarrow k(n^2+2n+1-2n^2+n^2-2n+1) = -2$$
$$\Rightarrow 2k = -2 \Rightarrow k = -1,$$

giving as our general solution $v_n = A_1 + A_2 n - n^2$,$n = 0, 1, 2\cdots$.

10. Given the initial conditions that $v_0 = v_l = 0$ gives the equations $A_1 = 0$ and $A_2 l - l^2 = 0$ so that $A_2 = l$. Hence our particular solution is $v_n = ln - n^2 = n(l-n)$, $n = 0, 1, 2, \cdots$.

Problem Set 8

1.
$$g(x) = (x^2)^5(1+x+x^2+\cdots)^5 = x^{10}\big(\frac{1}{1-x}\big)^5$$

and so we require the coefficient of x^{r-10} in the expansion of $(1-x)^{-5}$. By putting $n=5$ in the given identity we obtain

$$\binom{r-10+5-1}{r-10} = \binom{r-6}{r-10} = \frac{(r-6)(r-7)(r-8)(r-9)}{24}$$

.

2. Here we want the coefficient of $x^{8-2} = x^6$ in $(1-x)^{-10}$; putting $r=6$ and $n=10$ then gives:

$$\binom{6+10-1}{6} = \binom{15}{6} = \frac{15\times 14\times 13\times 12\times 11\times 10}{6\times 5\times 4\times 3\times 2} = 5005.$$

3. Our generating function here is $(1+x+x^2+\cdots)^2(1+x^2+x^4+\cdots) = (1-x)^{-2}(1-x^2)^{-1}$. The generating functions in this product are respectively

$$\sum_{r=0}^{\infty}\binom{r+2-1}{2}x^r = \frac{1}{2}\sum_{r=0}^{\infty}(r+1)(r+2)x^r,\ \sum_{r=0}^{\infty}x^{2r},$$

Denoting the corresponding coefficients by a_i and b_i, we require $a_0b_{10} + a_1b^9 + \cdots + a_{10}b_0$. Since $b_{2i+1} = 0$ and $b_{2i} = 1$ this simplifies to $a_0+a_2+a_4+a_6+a_8+a_{10}$. Hence we obtain

$$1 + 6 + 15 + 28 + 45 + 66 = 161.$$

4. Here we want the coefficient of x^{12} in the product

$$g(x) = (1 + x + x^2 + x^3 + x^4)^5 = (\frac{1-x^5}{1-x})^5$$

$$= (1 - \binom{5}{1}x^5 + \binom{5}{2}x^{10} + \cdots)(1 + \binom{5}{1}x + \binom{6}{2}x^2 + + \binom{r+4}{r}x^r + \cdots)$$

so the required coefficient is

$$\binom{16}{12} - \binom{11}{7}\binom{5}{1} + \binom{5}{2}\binom{6}{2} = \frac{16 \cdot 15 \cdot 14 \cdot 13}{24} - 5\frac{11 \cdot 10 \cdot 9 \cdot 8}{24} + 10 \cdot 15$$

$$= 1820 - 1650 + 150 = 320.$$

5. In this case $g(x) = (1+x)^{19}(1+x+x^5)$ and we require the coefficient of x^{15}. Again this has the form $a_0b_{15} + a_1b_{14} + \cdots + a_{15}b_0$. However, $b_0 = b_1 = b_5 = 1$, all other $b_i = 0$. Hence we require just

$$a_{15} + a_{14} + a_{10} = \binom{19}{15} + \binom{19}{14} + \binom{19}{10}.$$

6. Here we require the coefficient of x^{25} in the generating function:

$$g(x) = (1 + x + x^2 + \cdots + x^{10})(1 + x + x^2 + \cdots)^6 = (1-x)^{-7} \cdot (1 - x^{11});$$

in this case this gives a sum of products of the form

$$a_{14}b_{11} + a_{25}b_0 = \binom{25+7-1}{25} - \binom{14+7-1}{14} = \binom{31}{25} - \binom{20}{14}.$$

7. Here we require the coefficient of x^{25} in the generating function

$$g(x) = (x^2 + x^3 + x^4 + x^5 + x^6)^7 = x^{14}(1 + x + x^2 + x^3 + x^4)^7;$$

so we just need the coefficient of $x^{25-14} = x^{11}$ in

$$(\frac{1-x^5}{1-x})^7 = (1 - \binom{7}{1}x^5 + \binom{7}{2}x^{10} + \cdots)(1 + \binom{1+6}{1}x + \cdots + \binom{r+6}{r}x^r + \cdots)$$

which is

$$\binom{17}{11} - 7\binom{12}{6} + \binom{7}{2}\binom{7}{1}.$$

8. Again it's the coefficient of x^{25} this time in

$$g(x) = (x + x^2 + \cdots + x^6)^{10} = x^{10}(1 + x + \cdots + x^5)^{10},$$

which is the coefficient of $x^{25-10} = x^{15}$ in

$$\Big(\frac{1-x^6}{1-x}\Big)^{10} = (1-x^6)^{10}(1+\binom{1+9}{1}x+\cdots+\binom{r+9}{r}x^r+\cdots)$$

which is

$$\binom{24}{11} - 10\binom{18}{9} + \binom{10}{2}\binom{14}{5}.$$

9. The exponential generating function is in this case

$$g(x) = (x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots)^3 = (e^x - 1)^3.$$

The coefficient of x^r in this case is the number of ways of putting r distinct objects into 3 distinct rooms in a particular order. Since we are not interested in the order in which the people enter the room in our problem, our answer will in general be $\frac{a_r}{r!}$. Continuing we have

$$g(x) = e^{3x} - 3e^{2x} + 3e^x - 1 =$$

$$= \sum_{r=0}^{\infty} 3^r \frac{x^r}{r!} - 3\sum_{r=0}^{\infty} 2^r \frac{x^r}{r!} + 3\sum_{r=0}^{\infty} \frac{x^r}{r!} - 1$$

$$= \sum_{r=0}^{\infty} (3^r - 3\cdot 2^r + 3)\frac{x^r}{r!} - 1;$$

in particular, the coefficient of $\frac{x^{25}}{25!}$ is $3^{25} - 3\cdot 2^{25} + 3$.

10. The exponential generating function for this problem is

$$g(x) = (1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots)(x + \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots)(1 + x + \frac{x^2}{2!} + \cdots)^2$$

$$= \frac{1}{2}(e^x + e^{-x})\frac{1}{2}(e^x - e^{-x})e^x e^x$$

$$= \frac{1}{4}(e^{2x} - e^{-2x})(e^{2x}) = \frac{1}{4}(e^{4x} - 1).$$

It is the exponential generating function that is required as the ordering of the repetitions of a particular digit within a particular choice of set of places for that digit does not matter. Hence we require the coefficient of $\frac{x^r}{r!}$ in $g(x)$, which is $\frac{1}{4}\cdot 4^r = 4^{r-1}$.

Problem Set 9

1. Let A_1 be the set of hands with a void in spades, and similarly define A_2, A_3 and A_4. We have $N = \binom{52}{5}$ and $|A_i| = \binom{39}{5}$, $|A_iA_j| = \binom{26}{5}$, $|A_iA_jA_k| =$

$\binom{13}{5}$ while a void in all suits is impossible. Hence we obtain:

$$|\bar{A}_1\bar{A}_2\bar{A}_3\bar{A}_4| = \binom{52}{5} - 4\binom{39}{5} + 6\binom{26}{5} - 4\binom{13}{5}.$$

Comment In general, S_k is a sum of $\binom{n}{k}$ different k-tuple intersections of the n A_i's. To find $|A_1 \cup \cdots \cup A_n|$ we just note that this set is the complement of the intersection of the complements and so

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = S_1 - S_2 + S_3 - \cdots + (-1)^n S_n.$$

2. Here we have $N = 6^{10}$. Let A_i denote the set of rolls in which the number i does not appear, $1 \leq i \leq 6$. Then $|A_i| = 5^{10}$, and $S_1 = 6 \cdot 5^{10}$. Next $|A_iA_j| = 4^{10}$ and so $S_2 = \binom{6}{2}4^{10}$. In general $|A_{i_1} \cdots A_{i_t}| = (6-t)^{10}$ so that $S_t = \binom{6}{t}(6-t)^{10}$. Hence

$$|\bar{A}_1 \cdots \bar{A}_6| = 6^{10} - 6 \cdot 5^{10} + 15 \cdot 4^{10} - 30 \cdot 3^{10} + 15 \cdot 2^{10} - 6.$$

3. Here we have $N = 10^n$. Let A_i be the set of sequences in which i is absent $(i = 1, 2, 3)$. Then $S_1 = 3 \cdot 9^n$, $S_2 = 3 \cdot 8^n$ and $S_3 = 7^n$ and we have

$$|\bar{A}_1\bar{A}_2\bar{A}_3| = 10^n - 3 \cdot 9^n + 3 \cdot 8^n - 7^n.$$

4. Let A_i be the set of distributions with a void in box i $(1 \leq i \leq 5)$. Here we require to know $|A_1 \cup \cdots \cup A_5| = S_1 - S_2 + S_3 - S_4 + S_5$. In general, $S_t = \binom{5}{t}(5-t)^r$ so we obtain:

$$5 \cdot 4^r - 10 \cdot 3^r + 10 \cdot 2^r - 5.$$

5. We require the coefficient of x^{20} in the generating function

$$g(x) = (1 + x + x^2 + \cdots + x^8)^6 = (\frac{1-x^9}{1-x})^6$$

$$= (1 - 6x^9 + \binom{6}{2}x^{18} - \cdots)(1 + \binom{6}{1}x + \cdots + \binom{r+5}{r}x^r + \cdots),$$

so the required coefficient is

$$\binom{25}{20} - 6\binom{16}{11} + 15\binom{7}{2}.$$

6. Let our universe $\mathcal{U}$ be the set of all non-negative integer solutions and let A_i be the subset of integer solutions in which $x_i \geq 9$. Hence $N = |\mathcal{U}| = \binom{20+6-1}{20} = \binom{25}{20}$. Next $|A_i| = \binom{(20-9)+6-1}{20-9} = \binom{16}{11}$ and $|A_iA_j| = \binom{(20-9-9)+6-1}{20-9-9} = \binom{7}{2}$. Intersections of more than two of the A_i's are empty. Hence we again find our answer is

$$\binom{25}{20} - 6\binom{16}{11} + 15\binom{7}{2}.$$

7. Our universe is the set of all permutations on an n-set so that $N = n!$ Let A_i be the subset of solutions where lead i is correctly plugged into socket i. Then $|A_i| = (n-1)!$ and in general $|A_{i_1} \cdots A_{i_k}| = (n-k)!$ We see therefore that $S_k = \binom{n}{k}(n-k)!$ Hence we get

$$D_n = \sum_{k=0}^{n}(-1)^k \binom{n}{k}(n-k)! = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Hence the required probability is

$$D_n/n! = \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

8. Note that $\frac{D_n}{N} = 1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}$, which is the first $n+1$ terms of the series for $e^{-1} \approx 0 \cdot 366$. Since this alternating series converges very rapidly, for all but small n the proportion of derangements is very close to $\frac{1}{e}$.

9. Using the expression of Question 7 we get

$$nD_{n-1} + (-1)^n = n! \sum_{k=0}^{n-1} \frac{(-1)^k}{k!} + (-1)^n$$

$$= n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} = D_n.$$

.

10. To start the induction we note that $1 = D_2 = 1 \cdot D_1 + (-1)^2$ as $D_1 = 0$ so the recursion holds for $n = 2$. Using induction and then invoking Question 9 we then get for $n \geq 3$

$$(n-1)(D_{n-1} + D_{n-2}) = nD_{n-1} + (n-1)D_{n-2} - D_{n-1}$$

$$= nD_{n-1} + (D_{n-1} - (-1)^{n-1}) - D_{n-1} = nD_{n-1} + (-1)^n = D_n.$$

Comment Alternatively we can argue that the collection counted by the D_n is the union of two mutually exclusive types as follows. Given a derangement α of X_{n-1} choose $i \in X_{n-1}$ ($(n-1)$ choices) and define a derangement α' on X_n by putting $i\alpha' = n$, $n\alpha' = i\alpha$ and α, with α' agreeing otherwise. This process is one-to-one so this gives $(n-1)D_{n-1}$ derangements of X_n. Next, choose a point $i \in X_{n-1}$ ($(n-1)$ choices) and let α be a derangement of $X_{n-1} \setminus \{i\}$. Define a derangement α' of X_n by putting $i\alpha = n$ and $n\alpha = i$ with α and α' agreeing on $X_{n-1} \setminus \{i\}$. Again this process is also one-to-one so provides a further $(n-1)D_{n-2}$ derangements of X_n. Furthermore no derangement on X_n can arise from both of these processes and so pooling the two types gives a total of $(n-1)(D_{n-1} + D_{n-2})$ derangements of the n-set X_n. This exhausts all the derangements of X_n for any such derangement is the outcome of one of the other of these processes. Hence $D_n = (n-1)(D_{n-1} + D_{n-2})$.

Problem Set 10

1. By inspecting triangles, rectangles and pentagons we see that $C_1 = 1$, $C_2 = 2$ and $C_3 = 5$.

2. Label the vertices of the $(n+2)$-gon N by the integers $1, 2, \cdots, n$ and fix attention on the edge $E = 1\,2$. In any partition of N by non-intersecting triangles, E is the base of some triangle T_k, where k is the third vertex of T_k $(3 \le k \le n+2)$. The sides $1\,k$ and $2\,k$ split N into an $(n-k+4)$-gon and a $(k-1)$-gon respectively. Each of these can, independently of the other, be partitioned into C_{n-k+2} and C_{k-3} triangles, so the total number of ways this can be done is the product $C_{k-3}C_{n-k+2}$. Summing these products over k gives:

$$C_n = \sum_{k=3}^{n+2} C_{k-3}C_{n-k+2} = \sum_{k=1}^{n} C_{k-1}C_{n-k}.$$

3. The number of ways of choosing m balls from a collection of n red and m blue labelled balls is a sum, from $k = 0$ to $k = n$, of the number of ways of choosing k blue balls and $m-k$ red balls, which in symbols is:

$$\sum_{k=0}^{n} \binom{n}{k}\binom{m}{k} = \binom{n+m}{m}, \ (n \le m).$$

4. For $n = 1$ we have $\binom{2}{1} = 2 = \frac{(-\frac{1}{2})}{1!}(-4)^1$ to start the induction. Next assume the formula holds for some $n \ge 1$ and consider inductively the $(n+1)$ case:

$$\frac{(2(n+1))!}{(n+1)!(n+1)!} = \frac{(2n+2)(2n+1)}{(n+1)^2}\cdot\frac{(2n!)}{n!n!} = \frac{2(2n+1)}{n+1}\cdot\frac{(-\frac{1}{2})(-\frac{3}{2})\cdots(-\frac{2n-1}{2})}{n!}(-4)^n$$

$$= -\frac{2n+1}{2}\cdot\frac{(-\frac{1}{2})(-\frac{3}{2})\cdots(-\frac{2n-1}{2})}{(n+1)!}(-4)^n(-4)$$

$$= \frac{(-\frac{1}{2})(-\frac{3}{2})\cdots(-\frac{2n-1}{2})(-\frac{2(n+1)-1}{2})}{(n+1)!}(-4)^{n+1},$$

and so the induction continues, thus establishing the result.

5. We need to show that the coefficient of x^n in the expansion of $(1-4x)^{-\frac{1}{2}}$ matches that of the answer of Question 4. But by the binomial expansion we get:

$$(1-4x)^{-\frac{1}{2}} = \sum_{n=0}^{\infty} \frac{(-\frac{1}{2})(-\frac{3}{2})\cdots(-\frac{1}{2}-n+1)}{n!}(-4x)^n$$

and since $-\frac{1}{2} - n + 1 = \frac{-1-2n+2}{2} = -\frac{2n-1}{2}$ we see that the coefficients do indeed match.

6. The coefficient a_k of x^k in the series for $g(x) = \sqrt{1-4x}$ is $\binom{2k}{k}$. Hence the coefficient for x^n in $(g(x))^2$ is $a_0a_n + a_1a_{n-1} + \cdots + a_na_0$. On the other

hand the coefficient of x^n for the geometric series $(1-4x)^{-1}$ is 4^n. Hence we obtain the required identity in the form:

$$\sum_{k=0}^{n}\binom{2k}{k}\binom{2(n-k)}{n-k}=4^n.$$

7.

$$\sum_{n=0}^{\infty}\binom{2n}{n}\int_0^{\frac{1}{4}}x^{2n}\,dx=\int_0^{\frac{1}{4}}\frac{dx}{\sqrt{1-4x^2}}$$

$$\Rightarrow\sum_{n=0}^{\infty}\binom{2n}{n}\Big[\frac{x^{2n+1}}{2n+1}\Big]_0^{\frac{1}{4}}=\frac{1}{2}\int_0^{\frac{1}{2}}\frac{du}{\sqrt{1-u^2}}$$

$$\Rightarrow\sum_{n=0}^{\infty}\binom{2n}{n}\frac{1}{4^{2n+1}(2n+1)}=\frac{1}{2}\big[\sin^{-1}u\big]_0^{\frac{1}{2}}$$

$$\Rightarrow\sum_{n=0}^{\infty}\frac{1}{4^{2n}(2n+1)}\binom{2n}{n}=2\sin^{-1}(\frac{1}{2})=2\cdot\frac{\pi}{6}=\frac{\pi}{3}.$$

8.

$$(h(x))^2=\big(\sum_{k=0}^{\infty}C_kx^k\big)^2;$$

the coefficient of x^k in this square is $C_0C_k+C_1C_{k-1}+\cdots+C_kC_0=C_{k+1}$ by Question 2 . Therefore $(h(x))^2=\sum_{k=0}^{\infty}C_{k+1}x^k$.

9.

$$x(h(x))^2=\sum_{k=0}^{\infty}C_{k+1}x^{k+1}=\sum_{k=1}^{\infty}C_kx^k=h(x)-1$$

$$\therefore x((h(x))^2-h(x)+1=0.$$

Solving this as a quadratic in the unknown $h(x)$ gives

$$h(x)=\frac{1\pm\sqrt{1-4x}}{2x};$$

note that, for the positive sign, the limit as $x\downarrow 0$ of this expression is $+\infty$ while $C_0=1$. Hence it is the negative root (which has the correct limiting behaviour) that we want:

$$h(x)=\frac{1-\sqrt{1-4x}}{2x}.$$

10.

$$h(x)=\frac{1}{2x}\big(1-\big[1+\frac{(\frac{1}{2})}{1!}(-4x)+\frac{(\frac{1}{2})(-\frac{1}{2})}{2!}(-4x)^2+\frac{(\frac{1}{2})(-\frac{1}{2})(-\frac{3}{2})}{3!}(-4x)^3+\cdots\big]\big)$$

$$=\frac{1}{4x}\big(\frac{1}{1!}(4x)+\frac{(\frac{1}{2})}{2!}(4x)^2+\frac{(\frac{1}{2})(\frac{3}{2})}{3!}(4x)^3+\cdots+\frac{(\frac{1}{2})(\frac{3}{2})\cdots(\frac{2n-1}{2})}{(n+1)!}(4x)^{n+1}+\cdots\big)$$

$$= 1 + x + 2x^2 + \cdots + \frac{4^n \times 1 \times 3 \times 5 \times \cdots \times (2n-1)}{2^n (n+1)!} x^n + \cdots$$

$$\Rightarrow C_n = \frac{1}{n+1} \cdot \frac{2^n \times 1 \times 3 \times \cdots \times (2n-1)}{n!}$$

$$= \frac{1}{n+1} \cdot \frac{(2n)!}{(n!)^2} = \frac{1}{n+1} \binom{2n}{n}.$$